APSEA | Atlantic Provinces Special Education Authority

ASL Translation

Privacy Breach Protocol

What is privacy?

Privacy can be defined as the right of individuals to control the collection, use and disclosure of personal information about themselves.

This Privacy Breach Protocol outlines the key steps that must be taken when there is a known or suspected privacy breach affecting APSEA. This Protocol must be followed when completing a Privacy Breach Reporting Form.

What is a privacy breach?

A privacy breach occurs when personal information is accessed, collected, used, disclosed, retained, or destroyed in a matter inconsistent with the privacy provisions of the Access to Information and Protection of Privacy Act (ATIPPA), in Newfoundland and Labrador, the Right to Information and Protection of Privacy Act (RTIPPA) in New Brunswick, the Freedom of Information and Protection of Privacy Act (FOIPOP) in Nova Scotia, and the Freedom of Information and Protection of Privacy Act (FOIPOP) in Prince Edward Island.

Privacy breaches can take many different forms, including (but not limited to):

- Sending misdirected email or fax containing personal information;
- A loss of hard drives or physical files containing personal information;
- Inappropriate internal access to information by an employee;
- Loss or theft of mobile devices, including laptops, USB sticks;
- Hacking of computers, servers, and websites; and
- Phishing or social engineering attacks or malicious software (i.e., ransomware).

Who should you contact? (Internal Notification)

If you become aware of a privacy breach or a suspected privacy breach, immediately notify your direct supervisor (who will ensure notification of relevant breach response individuals internally, including the Director of Human Resources and their supervisor) and complete the APSEA Privacy Breach Reporting Form. If the breach involves criminal activity such as fraud or theft, the police should be notified.

Contain the Breach

Contain the breach as soon as possible to minimize harm. Suspend the activity or process that caused the breach as soon as possible, and if feasible, get the personal information back into your custody and control immediately.

If the breach is electronic in nature, contact the Manager of Information Technology (IT) and the Director of Finance and Administration, for direction on and assistance with breach containment.

Initial Investigation and Evaluation of Risk

A thorough investigation of the breach will allow for an evaluation of the risks relating to the breach, which will inform the breach response, including notifications.

The Director of Human Resources (or designate with appropriate authority to investigate) will work with you to investigate the breach (e.g., what happened, when, who is affected). Document exactly what happened and detail the steps taken to address the privacy breach.

Consider and document the following in assessing risk.

- What caused the breach? Was it accidental, internal, a bad actor, etc.?
- Is there a risk of ongoing exposure of the information?
- What is the extent of the breach? How many individuals are affected? Who are the affected individuals (students, employees, third parties)?
- Was information lost or stolen? If stolen, was it the result of a targeted breach?
- Was the information encrypted?
- Has the information been recovered?
- What steps have been taken to minimize harm?
- Is there a risk of identity theft or other harm?
- Is there harm to the public?

Notification

The Director of Human Resources or their designate will assist you in determining whether notification to individuals affected and the relevant privacy commissioner are appropriate, and if so, how to carry out proper notification, including ensuring all necessary information is included in the notification.

Corrective Measures and Lessons Learned

Take steps to reduce the risk of future breaches. APSEA will also assess what can be done to prevent such breaches from happening again and consider:

- conducting a security audit of both physical and technical security;
- reviewing system controls to ensure all necessary technical safeguards are in place;
- reviewing and updating policies as required.

MANY OF THE STEPS ABOVE MUST BE CARRIED OUT SIMULTANEOUSLY OR IN QUICK SUCCESSION.

Please Note: Depending on circumstances, APSEA may consider reporting privacy breaches to a provincial privacy office in the province where the breach occurs, and/or where information relates to individuals in a particular province. For example, a privacy breach that occurs in Newfoundland and Labrador (NL) but includes information relating to individuals in other provinces in addition to NL may be reported to all relevant Offices of the Information and Privacy Commissioner (OIPC).

The Access to Information and Protection of Privacy Act (ATIPPA) (NL), Right to Information and Protection of Privacy Act (RTIPPA) (NB), Freedom of Information and Protection of Privacy Act (FOIPOP) (NS), and Freedom of Information and Protection of Privacy Act (FOIPOP) (PEI) provide individuals a right to access records in the custody and control of a public body as well as protection of personal information by public bodies in the respective province.

Approved: February 2022
Reviewed/Revised: January 2024